

FEB 23 2011

Annual 47 C.F.R. § 64.2009(e) CPNI Certification Mail Room

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011 covering the prior calendar year 2010

Date filed: February 12, 2010

Name of company(s) covered by this certification: TelNet Worldwide, Inc.

Form 499 Filer ID: 822684

Name of signatory: Mark Iannuzzi

Title of signatory: President

Certification:

I, Mark Iannuzzi, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

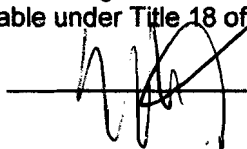
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

 2/12/11

Attachments: Accompanying Statement explaining CPNI procedures

Two copies rec'd 044
LJABODE

Attachment A: TelNet Worldwide CPNI Policies & Procedures

Overall Statement: TelNet Worldwide ("TelNet") is a telecommunications carrier subject to the rules and regulations set forth in 47 C.F.R. Section 64 of the Commission Rules. TelNet and its affiliates utilize reasonable and adequate safeguards and procedures to ensure compliance with the regulations pertaining to Customer Proprietary Network Information ("CPNI") found in 47 C.F.R. Section 64; including but not limited to: 1) employee training; 2) following "opt-out" notice rules; 3) electronic flagging of customer accounts; 4) password protection of account information; 5) seeking authorization and permission from customers prior to accessing customer information; and 6) adhering to internal compliance policies relating to customer privacy and information. Also, neither TelNet nor its affiliates sell any customer information to outside firms or vendors.

Specific Policies & Procedures: TelNet currently has the following specific policies and procedures in place to ensure compliance with the rules as stated above:

1. TelNet follows FCC rules relating to opt-out or opt-in notification.
2. Without customer approval TelNet does not use, disclose, or permit access to CPNI to provide or market service offerings outside of the category of services that the customer already purchases from TelNet. However, TelNet may use, disclose, or permit access to CPNI without customer approval for the following:
 - a. The provision of maintenance, repair and installation.
 - b. To market services formerly known as adjunct-to-basic services, such as but not limited to, speed dialing, computer provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain Centrex features; and
 - c. To protect the right or property of TelNet, or to protect the users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.
3. TelNet requires all TelNet Agents sign an Agent Agreement that specifies all customer information is proprietary to TelNet and all agents must comply with TelNet rules to keep such information confidential.
4. TelNet does not use CPNI information to identify or track customers who have called or switched to competing services.
5. TelNet informs customer of the precise steps that they must take to grant or deny access to CPNI.
6. TelNet stresses confidentiality of customer information at all times to TelNet employees. During initial employee training TelNet Human Resources trains all employees on privacy and methods of securing confidential information; this information is reiterated during annual employee training. In addition, all employees are provided a copy of the TelNet handbook which contains TelNet's policy on confidentiality of information. Violation of these procedures will subject personnel to disciplinary action which can include dismissal.
7. TelNet provides access to CPNI policies on its intranet so that all employees have access to the proper methods of maintaining CPNI confidentiality.
8. TelNet has developed internal policies for dealing with unauthorized access to CPNI and/or other confidential information; including policies for notification of customer and law enforcement.
9. TelNet has a specific policy regarding password management for employees with access to

T A

TelNet systems containing CPNI. TelNet requires log-on and password authentication each time an employee attempts to access TelNet customer databases. If log-in and password requirements are not met then access to the TelNet systems are denied.

10. TelNet has developed a policy for internal employees to deal with account confidentiality which sets forth when employees can use, disclose or give access to information regarding customers' accounts. Its objective is to identify the person inquiring or making a change to an account and to verify that person's authority to access the account in an effort to protect TelNet customer's rights to privacy.
11. When fielding a request from a privileged caller (an attorney, law enforcement, etc...), all such requests are immediately sent to TelNet Compliance Department personnel. Compliance personnel will review each such request and requires proper documentation before detailed information is released.